(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2001 (02.08.2001)

PCT

(10) International Publication Number
WO 01/55850 A1

(51) International Patent Classification[7]: G06F 01/24

(21) International Application Number: PCT/US01/02833

(22) International Filing Date: 24 January 2001 (24.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/490,941 25 January 2000 (25.01.2000) US

(71) Applicants and
(72) Inventors: **CZAJKOWSKI, David** [US/US]; 332 Alviso Way, Encinitas, CA 92924 (US). **GUDAITIS, Bernard** [US/US]; 1241 Via Landeta, Palos Verdes, CA 90274 (US).

(74) Common Representative: **CZAJKOWSKI, David**; 332 Alviso Way, Encinitas, CA 92924 (US).

(81) Designated States *(national)*: AU, CA, IN, JP, MX.

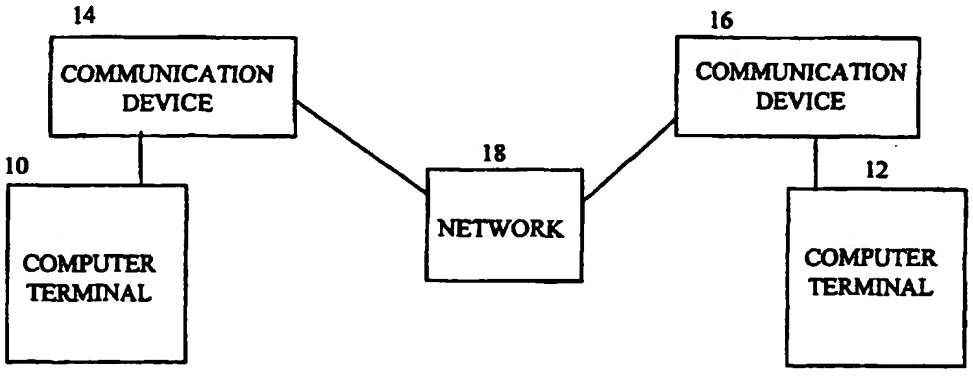
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/55850 A1

(54) Title: ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE



(57) Abstract: A method and apparatus for providing multiple layer encrypted Internet, Intranet, or e-mail communication device (14) communications. In particular, the process of encrypting Internet (18), Intranet, or e-mail messages with encryption algorithms embedded in integrated circuits incorporated into the communication device (14), with access to the encrypting circuit requiring a validation of a randomly generated cypher key and an user defined password.

TITLE: ENCRYPTED INTERNET AND INTRANET COMMUNICATION DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

BACKGROUND – FIELD OF INVENTION

This present invention relates a method for providing a secure encrypted computer communication channel across the Internet, more particularly, the use of e-mail access software and the addition of an integrated circuit embedded with several encryption algorithms to a communications device, thereby providing encryption/decryption capabilities.

BACKGROUND – DESCRIPTION OF PRIOR ART

Typical communication between two or more parties through the Internet 18 using a computer, 10 and 11 is accomplished through the use of a communications devices, 14 and 16 and communication software as referenced in FIG 1. A computer with communication capabilities, as reference in FIG 2 will utilize a communication controller 20 to interface with the Internet 22. The Internet consists of many public domain computers, electronic routers and switches, and computer servers generally accessible by the public. Accessing this network is not controlled by any individual organization and is not limited in any ways other than by protocol definitions (TCP, IP, etc).

Communication on the Internet between two parties can take place using two different methods:

1. *Sending data*: when one party groups a message and/or data package into a specific formatted sequence, attaches the Internet address, termed an Internet Protocol (IP) Address and then sends the message and IP Address to the Internet. The data is typically packetized using commercially available software and sent from the computer through the communication device onto the Internet.
2. *Accessing data*: when one party connects to a public or private database across the Internet by connecting to the database's website. Access is typically made by using the communication device to connect to the website's URL Address.

Originally, the security of these communications was not an issue as very few individuals possessed the necessary computer hardware or technical expertise to intercept the messages. However, the arrival of inexpensive personal computers and the explosion in the popularity of the Internet, in particular electronic commerce (e-commerce), prompted the development of computer communication security devices.

The existing method of security that presently exists is computer software programs that encrypt communication data between two users using encryption algorithms, such as the Blowfish algorithm. U.S. Pat. No. 6,014,444 relies an cypher key approach for encryption. These methods involve using a key, known by both the sender and receiver, which is used by the encryption algorithm to encode the data into an unrecognizable format.. The data is then passed from the sender to the receiver. After successful transmission, the receiver has an encrypted data package. The receiver must then get the key from the sender and use it to re-run the same decryption algorithm to decrypt the message. An example of this software is found in the 1999 PC Guardian Incorporated "Encryption Plus for Email" product datasheet.

The security of these software encryption systems may be compromised as the software (therefore the encryption algorithm) may be subject to computer hacking. Furthermore, the myriad of encryption software has led to incompatibilities. One encryption program is generally incompatible with a competing company's software. Therefore, the sender and the receiver must be using the same program. Lastly, once the encryption algorithm has been compromised, messages encrypted with the algorithm may easily decrypted. A person located external to the communications network may intercept and decrypt the message if the software has been effectively "hacked".

A different security approach has involved the use of computer smart cards. U.S. Pat. No. 5,761,306 provides other improved methods of encryption involving a system of computers to exchange public keys over an insecure network. These systems rely on a combination of nodes that are implemented by a computer, smart card, a stored data card in combination with a publicly accessible node machine. This system, however, will still depend on the effectiveness of the underlying encryption software and require the user to possess a smart card to effectively operate. Additionally, these software encryption systems generally only provide single layer encryption, in that the entire message will be encrypted using one algorithm.

U.S. Pat. No. 5,835,603 describes a home banking system using an encrypted modem as part of its system. This system is similar to all standard encryption techniques, but differs from the present invention in that it does not specify asymmetric and symmetric encryption functions embedded into an integrated circuit. Additionally, it does not utilize an Internet IP Address as part of its encryption system and does not offer any solutions for decryption.

Therefore, it is further desirable to have the encryption algorithm encoded onto a integrated circuit within the communication device. As such, hacking into the encryption chip would require purchasing an encryption chip and reverse engineering the chip to the underlying physical operations. In addition, for a large number of electronic network users, the private keys should be securely transmitted over the network.

SUMMARY

The present invention discloses an apparatus and method for providing secured information exchange through the Internet and Intranet, consisting of a computer communications device containing an integrated electronic circuit embedded with asymmetric and symmetric encryption/decryption algorithms.

According to the present invention, furthermore, there is provided a multiple step process which is added to existing standard Internet communication sequences for both sending and accessing data to implement the encryption procedure.

Other features of the present invention will become apparent from the accompanying drawings and from the detailed description which follows.

OBJECT AND ADVANTAGES

The present invention provides advantages over existing prior art in that:

(a) The inclusion of a hard wired integrated circuit containing embedded encryption algorithms into the computer communication device provides increased security over current software encryption systems. One wishing to discover the encryption algorithm would be required reverse engineer the chip down to the operational level (examine the gates and transistors comprising the chip function), as opposed to external program hacking to which a software-only system is susceptible. Such an effort would not generally be cost effective.

(b) Secure automatic electronic private key transmission between sender and receiver.

(c) The communication device with the integrated circuit, when installed in a computer, contains all the encryption hardware and software. No additional encryption technology is required to be purchased and installed.

(d) The process accompanying the present invention when incorporated to existing Internet communication sequences will require verification of the receiver's Internet or IP address before transmitting the encrypted data. Current systems do not require verification of the recipient's Internet or IP address.

BRIEF DESCRIPTION OF THE DRAWING

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals indicate similar elements and in which:

FIG 1 is a block diagram of a typical communication network.

FIG 2 is a block diagram of a computer with a communications device.

FIG 3 is a block diagram of an encryption/decryption communication device in accordance with an embodiment of the present invention.

FIG 4 is a flow chart of the encryption/decryption method in accordance with an embodiment of the present invention.

DETAILED DESCRITPION OF THE PRESENT INVENTION

The present invention contains all the functions necessary for secure communications in one physical device as referenced in figure 3. This device contains an encryption and decryption integrated circuit 30 that uses a combination of asymmetric and symmetric functions to encrypt and decrypt data. The encryption/decryption integrated circuit can be accessed by the user through a password protected user interface controller 32. This communication device also contains a signal processor 34 used to process the incoming and outgoing data. This may include multiplexing, de-multiplexing, modulating, demodulating, encoding, decoding, and error detection and correction. Memory 36 is included within the device for algorithm, control, and data storage. A network interface 38, electrical power 40, and a clock for internal timing 42 is also part of the communication device.

The present invention involves a multiple step process which is added to existing standard Internet communication sequences for both sending and accessing data. A primary private key is encrypted using a public/private key pair, then the remainder of the data is encrypted with a faster algorithm using another randomly generated primary key. An Encrypted Internet Communication System is required at both the sender and receiver for successful secure transmission. The verification process is completed using a set of software and hardware verification steps that unlock the encryption algorithm hardware to the receiver. The process involves a communication setup, a sender sequence and a receiver sequence. The process is as follows:

Communication Setup

When the communication device and associated software is installed into the computer, the following sequence is followed to setup levels of security:

1. The software requests a password from the user, either the sender or receiver.
2. The software converts the password to a digital, electronic bit format and transfers the digitized password to the communication device hardware, which stores the password permanently into a non-volatile hardware register.

Send Sequence

1. To access the encryption algorithm, the user must successfully re-enter the password into the software and matched in the hardware during the send sequence 44.
2. Sender requests encryption access from software.
3. Software asks for password from sender. (Steps 3 and 4 are optional).
4. Software compares password with previously stored password during the Communication Setup sequence of communication system. If matched, encryption algorithm is made available to sender. If not matched, encryption algorithm is not made available to sender. (Steps 3 and 4 are optional).
5. Data is passed through encryption hardware in communication device. The data encryption is performed in the following manner as referenced in figure 4:

a. the communication device accesses the receiver's public key. A Certification Authority (CA) is used to verify the receiver's public key 46.
b. the sender randomly generates its private key 48
c. the sender's private key is encrypted using the receiver's public key 50
d. the sender's data is encrypted using the sender's private key 52
e. the receiver's Internet Protocol's (IP) address is acted upon in one of the following ways:
i) the receiver's IP address is not encrypted
ii) a copy of the receiver's IP address is encrypted using a private key (different private key from the one encrypting the message) 54
f. the IP address, encrypted copy of the IP address (if ii is performed), encrypted private key, and encrypted message is transmitted as a message block to the receiver. If the IP address is encrypted the message block could be sent to the receiver through a private network to verify the receiver. If the IP address is not encrypted, the message block is sent to the receiver through normal channels 56.

Receive Sequence

1. After message data received by receiver, receiver requests software to de-encrypt data 58.
2. Software requests a password to communication device; receiver enters password.
3. Software transfers receiver password to communication device. Compare of password is completed by communication device. If matched, de-encrypt sequence is allowed to continue. If not matched, sequence is halted and error message is passed back to software.
4. Software then sends a un-encrypted e-mail on to the Internet through the communication device that provides a return message to the same (receiver) IP Address. The message will include a unique code to signify a verification check (unique verification code) and the IP Address. Numerous techniques can be used to verify the e-mail has reached the actual Internet, such as, use of "Certification Authority", reading the Domain Name Server and returning verification data and/or use of a private server that provides a return of the e-mail with verification of reaching the Internet. In all cases, the message will return to the receiver IP Address along with the unique verification code.
5. If the receiver's IP address is verified then the encryption of the data can proceed.
6. Software then transfers data to communication device.
7. The receiver's private key (as part of its private/public key pair) is then used to decrypted the sender's private key 60.
8. Then the receiver uses the sender's private key to decrypt the message 62.
9. The receiver's communication device deletes the sender's private key 64.
10. The receiver's communication device sends a message receipt to the sender 66.

CONCLUSIONS, RAMIFICATIONS, AND SCOPE OF INVENTION

Accordingly, the reader will see that the present invention provides multiple layer of encryption, yet will not impinge on the operational utility of the computer communications device. Furthermore, the apparatus and process outlined above prevents or efficiently deters external computer theft of sensitive information. Lastly, the apparatus and process may be upgraded with the addition of different algorithms.

While the above description contains many specifications, these specifications should not be construed as limitations on the scope or utility of the invention, but are presented to exemplify a preferred embodiment thereof.

Accordingly, the scope of the invention should be determined not by the embodiments presented, but by the appended claims and their legal equivalents.

CLAIMS

1. An apparatus for efficient encrypting and decrypting Internet or e-mail messages, comprising:

an integrated electronic circuit, said circuit physically located within a computer modem;

said circuit embedded with a common digital bit array;

said circuit embedded with a private signature cypher key;

said circuit embedded with asymmetric encryption algorithms;

said circuit embedded with symmetric encryption algorithms;

said circuit embedded with asymmetric decryption algorithms;

said circuit embedded with symmetric decryption algorithms.

2. An apparatus as recited in claim 1, wherein said circuit is located external of said computer modem, and means for connecting said externally located circuit to said modem.

3. A process to permit access to said encryption and decryption circuit recited in claim 1, wherein user access to said circuit further comprises:

means for converting multiple user defined passwords into digital bit arrays;

means for programming said digital bit arrays into a non-volatile register located within said circuit;

means for verifying future user request to access said circuit with said stored digital bit arrays;

means for permitting user access to said circuit upon verification of user defined password with stored digital bit arrays;

means for denying access to said circuit upon lack of verification of user defined password with stored digital bit array.

4. A process to bypass said encryption and decryption circuit recited in claim 1, comprising means for said computer communication device operating without accessing said circuit, thereby said communications device operating unencrypted.

5. A method of sending encrypting Internet or e-mail messages, comprising the steps of :

encrypting a message using an integrated circuit embedded with encryption algorithms,

said integrated circuit further embedded with a private signature cypher key;

said integrated circuit further embedded with a common digital bit array;

appending an encrypted message header to said encrypted message, said message header encrypted using a receiver's public encryption key;

said encrypted message header further comprising the sender's private signature cypher key and a common digital bit array;

means for transmitting said encrypted message header and said encrypted message to receiver over Internet;
means for transmitting said encrypted message header and said encrypted message to receiver over Intranet;
means for transmitting said encrypted message header and said encrypted message to receiver by e-mail.

6. A method of receiving and decrypting an encrypted message as recited in claim 5, comprising the steps of :

means for receiving an encrypted message header and encrypted message header and an encrypted message over Internet;

means for receiving an encrypted message header and encrypted message header and an encrypted message over Intranet;

means for receiving an encrypted message header and encrypted message header and an encrypted message by e-mail;

receiver gain access to decrypting integrated circuit as recited in claim 2;

means for integrated circuit to decrypt and validate common digital bit array located in message header;

means for integrated circuit to decrypt sender's private signature cypher;

means for sender's private signature cypher key to permit access to decrypting integrated circuit for decryption of message;

means for deleting sender's private signature cypher key from memory of receiver's computer;

means for preventing receiver from viewing, saving, copying, or retaining sender's private signature cypher key.

7. A method for efficient encryption and decryption of Internet or e-mail messages, comprising the steps of:

encrypting a message at a sending unit which is to be sent to a receiving unit using an integrated circuit embedded with algorithm located within said sending unit;

appending to the message at said sending unit the receiver's unencrypted IP address;

appending to said message the receiver's encrypted IP address;

said sending unit sends said encrypted message with said unencrypted IP address and said encrypted IP address;

receiving unit with an integrated circuit embedded with an encryption algorithm located within said receiving unit receives said encrypted message with said unencrypted IP address and said encrypted IP address using a receiving unit;

receiving unit decrypts said encrypted IP address, storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm located within receiving unit;

receiving unit stores said unencrypted IP address in a register built into said integrated circuit embedded with an encryption algorithm located within receiving unit;

means for comparing said register storing unencrypted IP address to said register storing decrypted IP address;

receiving unit decrypts said message if said register storing unencrypted IP address matches said register storing encrypted IP address;

means for halting decryption process if said register storing unencrypted IP address does not match said register storing encrypted IP address.

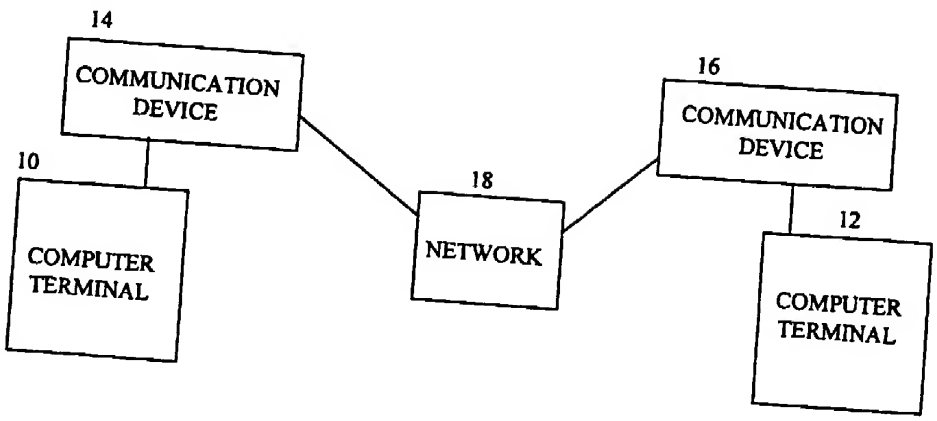


FIGURE 1 of 4 COMMUNICATION NETWORK

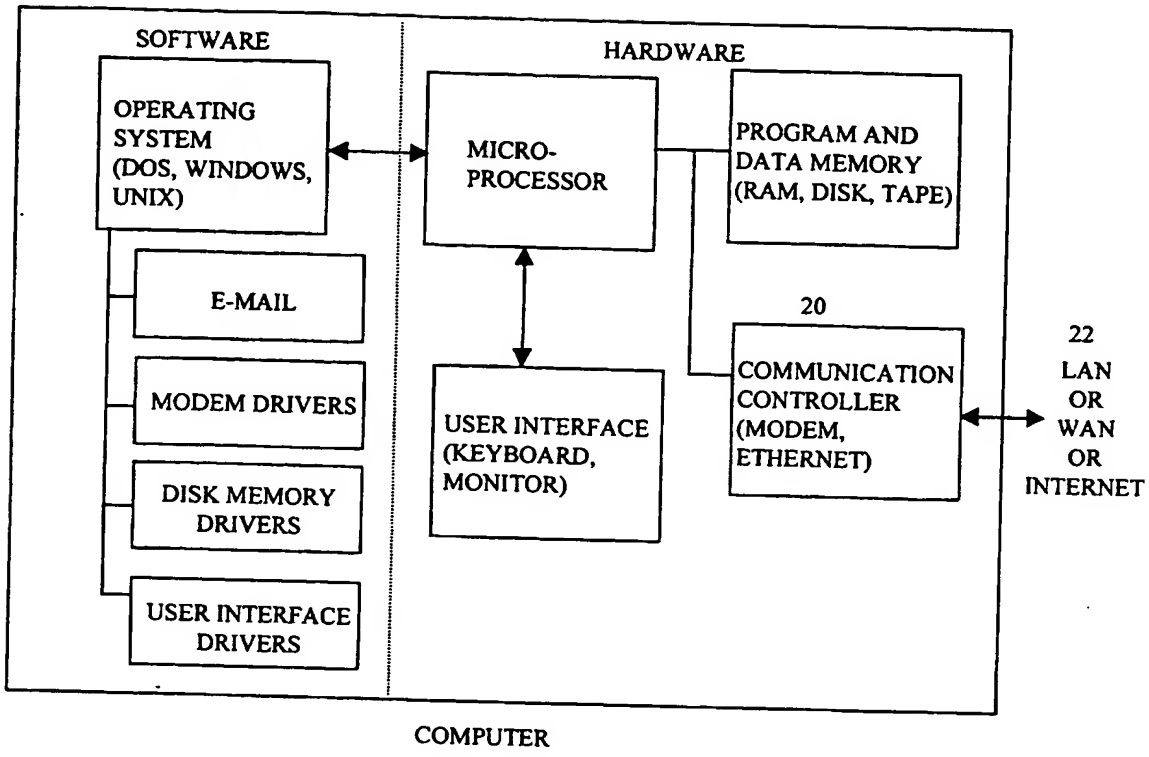


FIGURE 2 of 4 TYPICAL COMPUTER

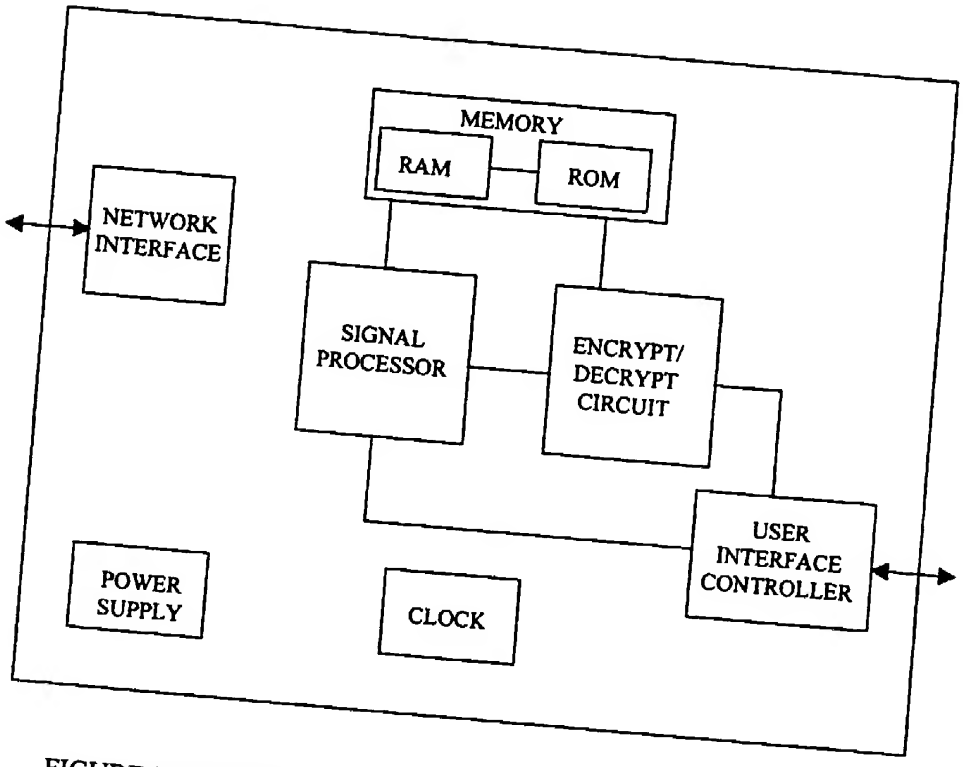


FIGURE 3 of 4 ENCRYPTION/DECRYPTION COMMUNICATION DEVICE

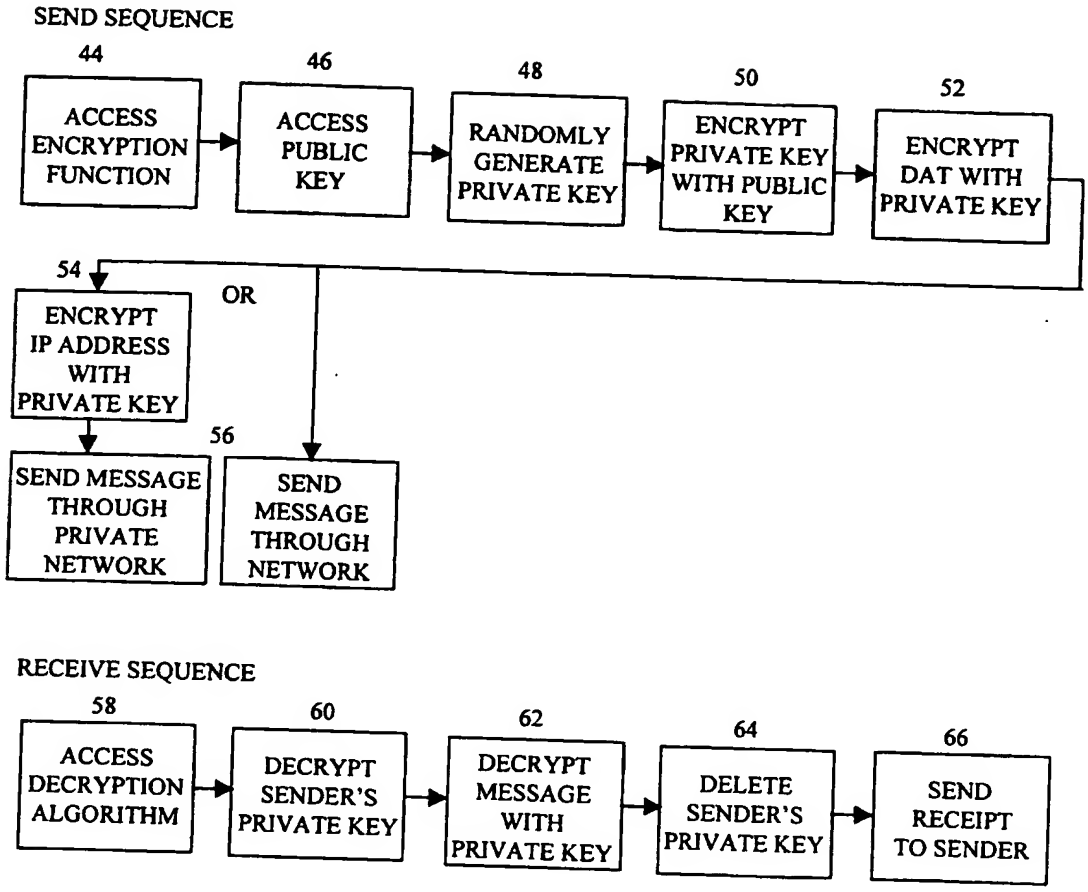


FIGURE 4 of 4 ENCRYPTION/DECRYPTION FLOW

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/02833

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 01/24
US CL : 713/182, 183, 184, 201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182, 183, 184, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
West

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,742,684 A (LABATON et al.) 21 April 1998, column 6, lines 57-66, column 7, lines 31-43, column 8, lines 35-41.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
15 May 2001 (15.05.2001)

Date of mailing of the international search report
14 JUN 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Thomas R. Peeso James R. Matthews
Telephone No. 703 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)